FEDERAL BUREAU OF INVESTIGATION
FOI/PA
DELETED PAGE INFORMATION SHEET
FOI/PA# 1204913-0

Total Deleted Page(s) = 11
Page 16 ~ b6; b7C; b7E;
Page 17 ~ b6; b7C; b7E;
Page 18 ~ b6; b7C; b7E;
Page 19 ~ b6; b7C; b7E;
Page 20 ~ b6; b7C; b7E;
Page 24 ~ b6; b7C; b7E;
Page 25 ~ b6; b7C; b7E;
Page 30 ~ b6; b7C; b7E;
Page 31 ~ b6; b7C; b7E;
Page 36 ~ b6; b7C; b7E;
Page 37 ~ b6; b7C; b7E;

XXXXXXXXXXXXXXXXXXXXXXXX
X Deleted Page(s) X
X No Duplication Fee X
X For this Page X
XXXXXXXXXXXXXXXXXXXXXXXX

(Rev. 01-31-2003)

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE **Date:** 10/08/2009

To: Cyber Division **ATTN:** Computer Intrusion Unit #2
SSA [redacted]

From: San Francisco
Squad CY-2/San Jose RA
Contact: SA [redacted]

Approved By: [redacted] b6 b7C

Drafted By: [redacted]

Case ID #: 288A-SF-~~NEW~~ 145486 (Pending) -1
288A-SF-NEW-GJ (Pending) -1

Title: ANTI-SEC;
UNSUB(S), et al;
IMAGESHACK - VICTIM;
COMPUTER INTRUSION

Synopsis: To Open Case and subfiles.

Details: On October 8, 2009, Special Agent (SA) [redacted] met with employees of IMAGESHACK located at 236 North Santa Cruz Avenue, Los Gatos, California, 95030, to discuss two recent computer intrusions of IMAGESHACK servers. IMAGESHACK is a company which provides internet image hosting. b6 b7C

IMAGESHACK advised SA [redacted] that the first computer intrusion occurred on July 10, 2009 at approximately 7 pm Pacific Standard Time (PST). A group by the name of ANTI-SEC gained access to one of the company database servers. The server the hacker(s) accessed contained [redacted] b6 b7C b7E The hacker(s) were also able to [redacted] In addition, the hacker(s) posted a message on the internet which claims the ANTI-SEC is a movement dedicated to the eradication of full disclosure. Their message further explained they plan to achieve this "through the full and unrelenting, unmerciful elimination of all supporters of full-disclosure and the security industry in its present form."

1 cm

b6
b7C [redacted]

OCA
10/09/09 DKS

OCA SA
10/08/09 dm
open GJ subfile dm

-145486

IMAGESHACK advised this computer intrusion affected approximately 50 million images and every user that was on their site at the time viewing images. IMAGESHACK is still not sure how the hacker(s) got into their database but believe [redacted] After this attack, they went through their servers [redacted] b6 b7C b7E

On August 2, 2009, IMAGESHACK believes the same hacker(s) came back and gained access to their servers again. IMAGESHACK has full and complete logs. It is apparent the hacker(s) [redacted] b6 b7C b7E

IMAGESHACK believes in the first computer intrusion in July 2009, the hacker(s) accessed one database [redacted] IMAGESHACK believes the hacker(s) [redacted] b6 b7C b7E IMAGESHACK estimates their losses at approximately $26,000.

It is requested that the following subfiles be opened:

Grand Jury SUB GJ

It is requested that the new case and subfiles be opened and assigned to SA [redacted] b6 b7C

♦♦

Title and Character of Case:

ANTI SEC
-

Date Property Acquired: 10/08/2009

Source from which Property Acquired:
IMAGESHACK, C/O [redacted], 263 N. SANTA CRUZ b6
263 N SANTA CRUZ AVE #100 b7C
LOS GATOS CA 95030

Anticipated Disposition:

Acquired By: [redacted]

Case Agent: [redacted]

Description of Property: Date Entered
1B 1

SIX(6) HARD DRIVES:
-THREE (3) WESTERN DIGITAL S/N WMAP41239964,S/N WMAKH1252071
AND S/N WMAKE2153028
-TWO(2) HITACHI S/N CKC4U9SE, S/N CKC5H4ME
-ONE(1) SAMSUNG S/N S09QJ1UL218644
ONE(1) HITACHI

Barcode: E4189643 Location: SJECR PRESS3 10/09/2009

* See 1A-4 for original FD-192. Evidence Returned e/f 4/30/12

Case Number: 288A-SF-145486
Owning Office: SAN FRANCISCO

288A-SF-145456-1B-1 sr.

Title and Character of Case:

ANTI SEC

Date Property Acquired: 08/19/2010

Source from which Property Acquired: SV-RCFL

Anticipated Disposition:

Acquired By: [redacted]

Case Agent: [redacted]

b6
b7C

Description of Property:

Date Entered

1B 2

ONE(1) CD LABELED SV-09-0162 (DERIVATIVE EVIDENCE OF 1B1)

Barcode: E4189947 Location: SJECR PRESS3 08/19/2010

* Evidence I.A'd. see 1A-3 for original FD-192 a.f. 4/27/11

Case Number: 288A-SF-145486
Owning Office: SAN FRANCISCO

WJM 8/24/2010

288A-SF-145486-1B-2

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 10/09/2009

On October 8, 2009, [redacted] was interviewed at his place of employment, IMAGESHACK, located at 236 North San Cruz Avenue, Suite 100, Los Gatos, California, 95030, telephone number 408-836-8579. After being advised of the identity of the interviewing agent, [redacted] provided the following information:

On July 10, 2009 at approximately 7:00 p.m., IMAGESHACK servers were hacked. The hacker(s) were able to get into the database server. This server contains [redacted] indicated the user passwords were [redacted] This sever also contained [redacted] indicated IMAGESHACK does not collect or maintain any credit card information [redacted] However, [redacted] stated the hacker(s) would have had [redacted] advised that from that server, the hacker(s) [redacted] Ultimately, the hacker(s) [redacted] advised this affected every user on site viewing images and approximately 50 million images. He indicated IMAGESHACK user images were replaced with this propaganda message for several hours. [redacted] said this caused quite a stir on the internet as it affected many website backgrounds as well. [redacted] advised a group named ANTI-SEC claimed responsibility for the hack of IMAGESHACK on the internet.

[redacted] said the technical team at IMAGESHACK believed the hack was a result of an [redacted] He advised that after the hack, the technical team at IMAGESHACK [redacted]

On August 2, 2009, [redacted] indicated the hacker(s) came back. He advised the staff at IMAGESHACK believes it was the same hacker(s) because they [redacted] advised that at the time it appeared the hacker(s) were [redacted] The technical team was able to [redacted]

b6
b7C
b7E

b6
b7C
b7E

Investigation on 09/08/2009 at Los Gatos, California

File # 288A-SF-145486-12 Date dictated NA

by SA [redacted]

b6
b7C

[redacted] believed the first hack affected approximately 490 IMAGESHACK servers. It appeared as though the hacker(s) [redacted]. In the first attack, the hacker(s) accessed [redacted]

b6
b7C
b7E

During the second attack, the hacker(s) went through the [redacted] then [redacted] and then [redacted] through there.

[redacted] advised during the first attack, [redacted] During the second attack, [redacted]

b6
b7C
b7E

He stated the estimated company losses are approximately $26,450.

[redacted] provided one Computer Disk (CD) labeled IMAGESHACK ANTISEC which he did not want returned that contained copies of an overview of the hacks, the ANTI-SEC jpg image posted to the servers, email from [redacted] regarding the identity of the hacker(s), and chat logs from IMAGESHACK staff during the August 2, 2009 attack.

[redacted] provided six hard drives to SA [redacted] and signed an FD-941 Consent to Search Computer(s) form for these six hard drives. [redacted] was also provided and signed an FD-597 United States Department of Justice, Federal Bureau of Investigation, Receipt For Property Received. The fd-941 and FD-597 and CD have been placed in a 1A envelope and sent to the file.

b6
b7C

(Rev. 05-01-2008)

CLASSIFIED BY NSICG/J9674T52
REASON: 1.4 (c)
DECLASSIFY ON: 08-28-2038
DATE: 08-28-2013

ALL INFORMATION CONTAINED HEREIN IS UNCLASSIFIED EXCEPT WHERE SHOWN OTHERWISE

(S) ~~SECRET~~//NOFORN/ [redacted] b1 b3

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE **Date:** 11/03/2009

To: San Francisco **Attn:** SA [redacted] CY-2
SA [redacted], CY-3

From: San Francisco
Oakland RA, I-2 and CY-3
Contact: [redacted] b6 b7C

Approved By: [redacted]

Drafted By: [redacted]

(S) **Case ID #:** [redacted] b1 b3
(U) 288J-SF-141890 (Pending)
(U) 288A-SF-145486 -3

(U) **Title:** ~~(S)~~ DEATH IS COMING FROM THE EAST;
UNSUB(S);
CI/CT - TNII

(U) ~~(S)~~ WORLD DEFACERS,
UNSUB(S);
CT - TNII
OO:SF

(U) ~~(S)~~ Anti-Sec
UNSUB(S);
IMAGESHACK - VICTIM

(U) **Synopsis:** ~~(S)~~ Identification of possible founding member of Anti-Sec.

~~**Derived From : FBI NSISCG-20090615**~~
~~**Declassify On:** 20341103~~

(S) **Reference:** [redacted]
(U) ~~(S)~~ 288A-SF-145486 Serial 1 b1 b3
(S) [redacted]

(S) ~~SECRET~~//NOFORN [redacted]

(S) ~~SECRET~~//NOFORN

To: San Francisco From: San Francisco
(S) Re: [redacted] b1 b3

(S) [redacted]

(U) Open source searches provide no information that Anti-Sec hacked [redacted]

(U) ~~(S//NF)~~ San Francisco division [redacted] b7E
[redacted] A hacking group named Anti-Sec gained access to one of the company's database servers and accessed [redacted] b6 b7C b7E. The hackers changed the server settings to redirect every image to a hacker logo. The hackers posted a message claiming that the Anti-Sec group is dedicated to the eradication of full disclosure by eliminating the cyber security industry. (288A-SF-145486, Serial : 1)

(U) Anti-Sec claimed that a [redacted]. An identified [redacted] further stated that Anti-Sec fabricated the claim of [redacted] b7E White-Hat Hacker and Cyber Security Communities. Open source research revealed that several large web hosting companies considered [redacted] (800A-HQ-C1591622-NOADMIN, Serial : 20010).

(U//FOUO) Anti-Sec is discussed in [redacted] b7E (800A-HQ-C1591622-NOADMIN, Serial 20010)

(S) ~~SECRET~~//NOFORN b1 b3

(S)

To: San Francisco From: San Francisco
Re:

(S)

b1
b3

Possible Identification of a founding member

(S)

(S)

To: San Francisco From: San Francisco
Re: [redacted]
(S)

LEAD(s):

Set Lead 1: (Info)

SAN FRANCISCO

AT SAN JOSE

(U) Read and Clear.

♦♦

(Rev. 05-01-2008)

UNCLASSIFIED

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE **Date:** 11/10/2009

To: San Francisco

From: San Francisco
Squad CY2/San Jose RA
Contact: SA [redacted]

Approved By: [redacted]

Drafted By: [redacted]

b6
b7C

Case ID #: 288A-SF-145486 (Pending) 4

Title: ANTI-SEC;
UNSUB(S);
IMAGESHACK - VICTIM;
COMPUTER INTRUSION

Synopsis: To Report US Attorney Office concurrence for new case opening.

Details: On October 9, 2009, Special Agent (SA) [redacted] emailed Chief Assistant United States Attorney (AUSA) for the Computer Intrusion and Hacking Unit, [redacted] regarding concurrence for new captioned investigation. The email contained a summary of the case information. SA [redacted] was contacted telephonically and granted concurrence regarding captioned investigation and advised that AUSA [redacted] would be assigned the case.

b6
b7C

Attached and made a part of this document is the email to AUSA [redacted]

♦♦

UNCLASSIFIED

288A-SF-145486-4

FD-542 (Rev. 03-23-2009)

UNCLASSIFIED

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE **Date:** 11/13/2009

To: San Francisco

From: San Francisco
Squad CY2/San Jose RA
Contact: SA [redacted]

Approved By: [redacted] b6 b7C

Drafted By: [redacted]

Case ID #: 288A-SF-145486 (Pending) - 7

Title: ANTI-SEC;
UNSUB(S), et al;
IMAGESHACK - VICTIM;
COMPUTER INTRUSION

Synopsis: To Claim Statistics.

Details: On September 16, 2009, Special Agent (SA) [redacted] telephonically spoke to the victim company, Imageshack, regarding captioned matter and set a date to meet in person.

On October 8, 2009, SA [redacted] met with [redacted] of Imageshack and obtained the detailed information about the captioned computer intrusions. Possible subject(s) have been identified. b6 b7C b7E

On November 13, 2009, SA [redacted]

UNCLASSIFIED

288A-SF-145486 - 7

To: San Francisco From: San Francisco
Re: 288A-SF-145486, 11/13/2009

Accomplishment Information:

Number: 2
Type: CIP 2703(f) ORDER SERVED
ITU: CIP
ITU: LIAISON WITH OTHER AGENCY
Claimed By:
SSN:
Name:
Squad: CY2

Number: 2
Type: CIP SUBJECT IDENTIFIED
ITU: CIP
ITU: LIAISON WITH OTHER AGENCY
Claimed By:
SSN:
Name:
Squad: CY2

b6
b7C

Number: 2
Type: CIP VICTIM CONTACTED/INTERVIEWED
ITU: AGENT INTERVIEW
ITU: CIP
ITU: INDIVIDUAL/NON-INFORMANT
ITU: LIAISON WITH OTHER AGENCY
Claimed By:
SSN:
Name:
Squad: CY2

♦♦

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 12/09/2009

On December 8, 2009, Special Agent [redacted] received a facsimile from [redacted] The aforementioned facsimile had been attached and is made a part of this document.

b6
b7C
b7E

Investigation on 12/08/2009 at Campbell, California

File # 288A-SF-145486 Date dictated NA

by SA [redacted]

b6
b7C

FD-302 (Rev. 10-6-95)

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 03/02/2010

On January 23, 2010, Special Agent (SA) [redacted] received a response via facsimile to a [redacted]

The response was addressed to SSA [redacted] and referenced [redacted]

b6
b7C
b7E

The above referenced letter had been attached and is made a part of this document.

Investigation on 01/23/2010 at Campbell, California (via facsimile)

File # 288A-SF-145486 - 13 Date dictated NA

by SA [redacted] b6 b7C D61 [redacted] DD4 WB

This document contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is loaned to your agency; it and its contents are not to be distributed outside your agency.

FD-542 (Rev. 03-23-2009)

UNCLASSIFIED

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE **Date:** 01/14/2010

To: San Francisco

From: San Francisco
Squad CY2/San Jose RA
Contact: SA [redacted]

Approved By: [redacted]

Drafted By: [redacted]

b6
b7C

Case ID #: 288A-SF-145486 (Pending) -12

Title: ANTI-SEC;
UNSUB(S), et al;
IMAGESHACK - VICTIM;
COMPUTER INTRUSION

Synopsis: To Claim Statistics.

Details: On January 12, 2010, Special Agent (SA) [redacted]

b6
b7C
b7E

On October 8, 2009, Imageshack provided SA [redacted] with six hard drives and consent to search those hard drives.

UNCLASSIFIED

To: San Francisco From: San Francisco
Re: 288A-SF-145486, 01/14/2010

Accomplishment Information:

Number: 1
Type: CIP 2703(f) ORDER SERVED
ITU: CIP
ITU: LIAISON WITH OTHER AGENCY
Claimed By:
SSN:
Name:
Squad: CY2

b6
b7C

Number: 8
Type: CIP VICTIM CONTACTED/INTERVIEWED
ITU: CONSENSUAL SEARCH
Claimed By:
SSN:
Name:
Squad: CY2

♦♦

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 04/27/2012

On April 27, 2012, Special Agent [redacted] returned six hard drives to [redacted] at his place of employment IMAGESHACK, 236 Santa Cruz Avenue, Los Gatos, California, 95030. A copy of the signed FD-597 United States Department of Justice Federal bureau of Investigation Receipt for Property Received/Returned/Released/Seized had been placed in a 1A envelop and sent to the file.

b6
b7C

Investigation on 4/27/2012 at Los Gatos, California

File # 288A-SF-145486 14 Date dictated NA

by SA [redacted]

b6
b7C

(Rev. 05-01-2008)

UNCLASSIFIED

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE **Date:** 04/27/2012

To: San Francisco

From: San Francisco
Squad CY2/San Jose RA
Contact: SA [redacted]

Approved By: [redacted] 4/30/2012

Drafted By: [redacted] b6 b7C

Case ID #: 288A-SF-145486 (Closed) ✓ -05

Title: ANTI-SEC;
UNSUB(S), et al;
IMAGESHACK - VICTIM
COMPUTER INTRUSION

Synopsis: To Close Captioned Case.

Details: Assistant United States Attorney (AUSA) [redacted] and Special Agent (SA) [redacted] have discussed captioned investigation and its status on numerous occasions. On March 16, 2012, AUSA [redacted] inquired via email if captioned investigation could be closed. SA [redacted] advised that since there are no good subject internet protocol (IP) addresses and no good follow-up leads or information from current sources, captioned investigation should be closed.

The evidence obtained in this investigation did not derive enough probable cause to result in the identification of a subject for a prosecuteable offense. On April 18, 2012, SA [redacted] received a letter from the United States Attorney's Office stating that their office has closed the investigation. The abovementioned letter has been attached and is made a part of this document. b6 b7C

On April 27, 2012, SA [redacted] returned the hard drives provided by Imageshack as evidence in captioned case back to the victim company.

It is recommended that captioned case be closed and that the evidence collected on captioned case be destroyed and/or returned

close case
C-05
4/30/2012

UNCLASSIFIED

Closed
4/30/12
DS

To: San Francisco From: San Francisco
Re: 288A-SF-145486, 04/27/2012

pursuant to FBI policy. There are no pending leads or further investigation required on captioned case.

♦♦

U.S. Department of Justice

United States Attorney
Northern District of California

150 Almaden Boulevard, Suite 900
San Jose, California 95113

DD: (408) 535-5061
FAX:(408) 535-5066

April 18, 2012

[redacted]
Special Agent
Federal Bureau of Investigation
1919 S. Bascom Avenue, Suite 400
Campbell, CA 95008

b6
b7C

RE: ImageShack Intrusion

Dear Special Agent [redacted]

This letter is to confirm that my office has closed the investigation into the ImageShack intrusion by a group known as Anti-Sec. Based on our conversations, you have conducted an exhaustive investigation and have been unable to identify the individual responsible for the intrusion. If you find new evidence, please resubmit the case for prosecution.

I appreciate all of your work on the case. Please do not hesitate to contact me if you have any questions. I can be reached at [redacted]

Very truly yours,

MELINDA HAAG
United States Attorney

[redacted]
Assistant United States Attorney